iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55238

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

NANO-AES Security Algorithm for Image Cryptography

Tejashwini C Kurbet[1], Jenitta J[2]
[1]*Department of ECE,* [2]*Senior member of IEEE, AMC Engineering College, Bangalore, India*

Abstract: ***Data transmission security is now essential in any wireless communication. The fundamental problem in wireless communication is ensuring the security of data transfer from source to destination through data encryption and decryption. We give a literature review on the security of the encryption AES method and its contemporary applications in communication, data transfer, and wireless communication in this study. To provide security, we employ the Advanced Encryption Standard (AES), which works with 128-bit data and encrypts it with 128-bit keys. In this paper, we will conduct a literature review of AES algorithms and pick AES algorithms for wireless communication applications, as well as design a Verilog AES subblock add round key, mix column, and s-box for a Spartan3 FPGA device using Xilinx ISE 9.1i software***
Keywords: Advanced Encryption System (AES), S-box, Spartan3 FPGA

I. INTRODUCTION

Information and communication are protected by the use of codes in cryptography, ensuring that only the intended audience may access and utilize the data. This system is a fashion used to render communication. The philanthropist can view the translated communication only by decrypting it with the correct code and keys. Cryptography is mainly used for the transmission of secured information across the computer network. A clear textbook paper is turned into a crypto textbook through the process of encryption by applying a significant and fine algorithm to it. Cryptography textbooks state that a document cannot be deciphered unless the anthology has access to the key that can break the encryption. In 1997 the United States government's National Institute of Standards and Technology NIST launched a project to discover a replacement for the data encryption standards (DES). The fact that des was not secure due to improvements in data storage and retrieval was universally acknowledged. The aim of NIST was to specify a DES remedy that our federal agencies may utilize for non-military security of information activities. The fact that markable and other non-government drug users would benefit from the NIST's work would be widely endorsed as a usable standard, according to this statement. The AES algorithm for encryption is a block cipher data that uses many encryption cycles and a secret key a block cipher is an encryption technique that only encodes one block of information at a time. The block in typical AES encryption has a length of 128 bits or 16 bytes. The phrase "rounds" describes how the secret code divides the material into groups and encrypts it 10 to 14 times, based on the key's size. This is discussed in the Wikipedia page on AES encryption. AES is neither computer source code nor a program in and of itself. It's a great explanation of how to hide data. The original authors and also other persons have released source code execution of AES encryption as part of the encryption process AES encryption employs a single key. The key's length can range from 128 bits (16 bytes) to 256 bits (32 bytes). 128-bit encryption refers to the use of a 128-bit encryption key. The same key is utilized for both encryption and decryption in AES. It is critical to use difficult-to-decipher and to keep the encryption key secret. Some keys are generated by the software used for this specific activity. Another approach is to choose a key based on a passphrase. In proper encryption systems, a pass encryption is never used as an encryption key on its own.

II. LITERATURE SURVEY

[1] Lightweight encryption circuits are critical to ensure adequate information security in emerging millimetre-scale platforms for the Internet of Things, which must deliver moderately high throughput with strict area and energy budgets. This requires the use of specialized AES accelerators, as they offer orders of magnitude energy savings compared to microcontroller-based implementations. In this paper, we present the architectural exploration of lightweight AES accelerators with the goal of minimizing energy consumption. We also estimate the lower bound on the number of cycles per encryption in lightweight AES designs as a function of the number of available S-boxes. In combination with sub/narrow-threshold circuit techniques, we present a low-cost, extremely energy-efficient AES encryption core for cubic millimetre platforms. Our test chip achieves a high energy efficiency of 0.83 pJ/bit at 0.32 V, which outperforms state-of-the-art low-cost AES designs by a factor of 7.[2]

©IJRASET: All Rights are Reserved

Although cryptosystem designers often assume that secret parameters are manipulated in closed, trusted computing environments, Kocher et al. 1998 reported that microchips leak information that correlates with processed data and introduced a new type of attack that is fundamentally different from software and algorithm attacks. These attacks use leaks or side-channel information such as power consumption data, electromagnetic emissions, or computation time to determine the secret key. Although FPGAs are becoming increasingly popular for cryptographic applications, there are few articles evaluating their vulnerability to such attacks. In this work, we describe the principles of the differential power analysis (DPA) attack and show a practical and successful implementation of this attack against an FPGA implementation of the Advanced Encryption Standard (AES) algorithm. The results obtained in this work clearly show that DPA poses a serious threat to the implementation of encryption algorithms on SRAM-based FPGAs unless effective countermeasures are taken. [3] This article examines the vulnerability of software and hardware implementations of cryptographic algorithms to performance analysis attacks. A simulation-based experimental environment is built to collect performance data, and attacks are performed on two implementations involving single-bit differential performance analysis (DPA), multi-bit DPA, and correlation performance analysis (CPA). Experimental results show that the hardware implementation has less data-dependent power loss to defend against performance attacks. An improved DPA approach is also proposed. It uses the Hamming distance of intermediate results as a performance model and orders plain text inputs to distinguish performance traces with maximum probability.[4] The AES combined S-box is a single stretcher that is shared by both the AES encryption and decryption data pathways. Can Right's design, announced in 2005 is now the most compact implementation of the AES combined S Box/ reversed S-box. Since then, the research community has added various optimizations over the pure S-box but the combination S-box /reversed S-box has received minimal attention. We present a novel AES combination S-box inverse S-box design that is both smaller and quicker than the can-right design in this work. This is accomplished by proposing a new tower field and optimizing each block inside the combined architecture for that field. In terms of size and speed our complexity study and ASIC implementation results in CMOS STM 65nm And Nan-Gate 15 nm Technologies show that design surpasses the competition.[5] In this paper, they show that some intermediate values from the inner rounds can be exploited by using techniques such as fixing certain plaintext/ciphertext bytes. We give five general principles for DPA vulnerability of unprotected AES implementations and give several general principles for the DPA vulnerability of protected AES implementations. These principles indicate which operations of AES are vulnerable to first- and second-order DPA. To illustrate the principles, we attack the two implementations of AES that use two types of countermeasures to achieve high resistance to performance analysis and show that they are vulnerable even to DPA.[6] To enhance the security of edge computing, all data transmitted to and from edge devices and all data stored on edge devices must be encrypted. In particular, if the data transmitted or stored contains sensitive personal information, long-term protection over periods of ten or more years may be required, which can only be achieved with post-quantum cryptography. This article first gives a brief overview of post-quantum public-key cryptosystems based on difficult mathematical problems involving hash functions, error-correcting codes, multivariate quadratic systems, and lattices. The suitability of lattice-based cryptosystems for resource-constrained devices is then discussed, and efficient implementations for 8- and 32-bit microcontrollers are presented [7] This work describes novel high-speed architectures for implementing the advanced encryption standard AES algorithm in hardware. Unlike previous work that dependent on lookup tables to achieve the AES algorithms sub-byte and inv-sub-bytes transformations, the suggested architecture relies solely on combinatorial logic. As a result, the uninterruptible delay generated by lookup tables in the traditional techniques is avoided, allowing the benefits of sub-pipelining to be fully realized. Furthermore, composite-filled arithmetic is used to reduce area needs, and alternative inversion methods in subfield GF (2/sup/4) are compared. Also given is an efficient key expansion design suitable for sub-pipelining round units.[8] It is vital to ensure the security of sensitive data transmitted between devices. LDRs (low-resource devices) built for limited contexts are becoming more common. Lightweight block ciphers ensure LDR secrecy by balancing sufficient security with little resource overhead. SIMON is a simple block cipher designed for hardware implementation. The purpose of this study is to implement, optimize, and model the SIMON cipher design for LDRs with a focus on energy and power as essential variables for LDRs. FPGA (Field programmable gate array) Technology is used in various implementations. Scalar and pipeline design implementations are studied. Scalar implementations require 39% fewer resources and consume 45% less electricity according to the results. Pipeline systems have 12 times the throughput and 31% less power consumption.[9] We introduce a nano advanced encryption standard AES with a very low gate count the following measures help to attain a low gate count. First, for AES we repeat the area crucial circuits which are an 8-bit substitution box (S-box) circuit and a 32-bit mixed column circuit. Second, we use our data transmission architecture to cascade the input flip flops (FFs) so that the output of the mix column circuits is directly connected to the first 32-bit input FFs without the use of any additional multiplexer circuits. Third, by assigning the data sequence to the input FFs (During The S-box and mix columns procedures), The shift row operation is executed implicitly.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Fourth for the add round and key expansion operations, we employ independent XOR gates. Our design is targeted at applications with very small footprints, such as biomedical applications. [10] The exponential growth of Internet of Things (IoT) applications, such as smart ecosystems or e-health, has added more security threats. To defend against known attacks on IoT networks, multiple security protocols must be established between nodes. Therefore, IoT devices need to perform various cryptographic operations such as public key encryption and decryption. However, classical public-key cryptosystems such as RSA and ECC are computationally too complex to be implemented efficiently on IoT devices and are vulnerable to quantum attacks. Therefore, these cryptosystems will no longer be secure and practical after quantum computing is fully developed. In this paper, we propose InvRBLWE, an optimized variant for binary learning with errors over the ring (ring-LWE) that is provably secure against quantum attacks and highly efficient for hardware implementations.

TABLE I: Existing Method Of Nano Aes Security Algorithm For Image Cryptography

TITLE	AUTHORS/ RESEARCHERS	PROPOSED METHOD	PARAMETERS	ADVANTAGES AND DISADVANTAGES
AES Architectures for minimum-energy operation and silicon demonstration in 65nm with the lowest energy per encryption	Wenfeng Zaho, Yajun Ha, Massimo Allito	Native and non-native round computation and key expansion.	Area, clock cycles, energy	ADVANTAGES: • Low energy • Low cost • Reduces delay DISADVANTAGES: Increase in the area due to the native mix column blocks
A practical differential power analysis attack against an FPGA implementation of AES cryptosystem	Mehadi Masoomi, Massoud Masoumi, Mahmoud Ahmadian	DPA (differential power analysis) In DPA, an attacker uses a method called a hypothetical model of the attacked device. The quality of this model is dependent on the knowledge of the attacker.	SRAM-based Xilinx Spartan II, Power	ADVANTAGES: • Reduces the switching noise DISADVANTAGES: • Attacking the output of mix-columns is very costly.
Experimental Implementation of DPA Attacks on AES Design with Flash-based FPGA Technology	Najeh kamoun, Lilian Bossuet, Adel Ghazel	Mainly three different techniques for DPA attack data processing. a) Correlation Analysis b) Distance of meantest c) Maximum likelihood method	Flash-based FPGA	ADVANTAGES: Easy to manipulate DISADVANTAGES: • Suitable countermeasure for DPA attack is not defined.
New Area Record for the AES Combined S-box/Inverse S-box.	Arash Reyhani-Masoleh, Mostafa Taha and Doaa Ashmawy	S-box/inverse S-box Arithmetic computations and logic computations with ASIC implementation.	Area, Power	ADVANTAGES: • Faster • Low power consumption DISADVANTAGES: • Design is complex

Principles on the Security of AES against first and second-order Differential Power Analysis	Jiqiang Lu, Jing Pan, Jerry den Hartog	AES implementations without countermeasures, which are categorized by the location of the intermediate byte(s) exploited	Power, XOR gates	ADVANTAGES: • Very simple and easy to conduct DISADVANTAGES: • sophisticated attacks are not taken into account
Securing Edge devices in the post-Quantum Internet of things using lattice - Based Cryptography	Zhe Liu, Kim-Kwang Raymond choo, Johann GroBschadl	This method is based on mainly four categories Lattice-based cryptography Multivariate cryptography Hash-based cryptography Code based cryptography	Lattice based cryptosystem	ADVANTAGES: • High efficiency • Less communication cost • Small key size DISADVANTAGES: • Long-term protection of data is not possible
High-speed VLSI architectures for the AES Algorithm	Xinmiao Zhang	This architecture is based on pipelining, sub-pipelining and loop-unrolling	Xilinx ISE 5.1i	ADVANTAGES: • Reduced area • Increased speed DISADVANTAGES: • It cannot achieve higher speed if large number of FPGA devices are available
FPGA modeling and optimization of a SIMON lightweight block cipher (2019)	Saed Abed, Reem jaffal, Bassam jamil Mohd and Mohammad Alshayeji	The model SIMON cipher design for LRDs is implemented with two types Scalar and pipelined	8-bit AVR microcontrollers	ADVANTAGES: • Lightweight • Less energy and power consumption DISADVANTAGES: • It mainly depends on parameter variations, voltage threshold and logic family.
Low gate-count Ultra small area nano Advanced Encryption Standard (AES) design	A Shreedhar et al	Low gate count is achieved by the following means Area-critical circuits Cascading input FFs Shift row operation Using independent XOR gates	Cadence tool for layout implementation	ADVANTAGES: • Small area DISADVANTAGES: • More number of clock cycles

Post -Quantum Crypto processors optimized for Edge and Resource-constrained devices in IoT	Shahriar Ebrahimi, Siavash Bayat-sarmadi	The proposed method is invRBLWE which is an optimized variant for binary learning with errors over the ring. There are two different architectures to implement invRBLWE 1) A high-speed architecture 2) An ultra-lightweight architecture	FPGA, Crypto-processor, Processor	ADVANTAGES: • Low power consumption • Lightweight Architecture DISADVANTAGES: • It is not reliable for differential power Analysis (DPA) attacks and simple and differential fault attacks (SFA and DFA)

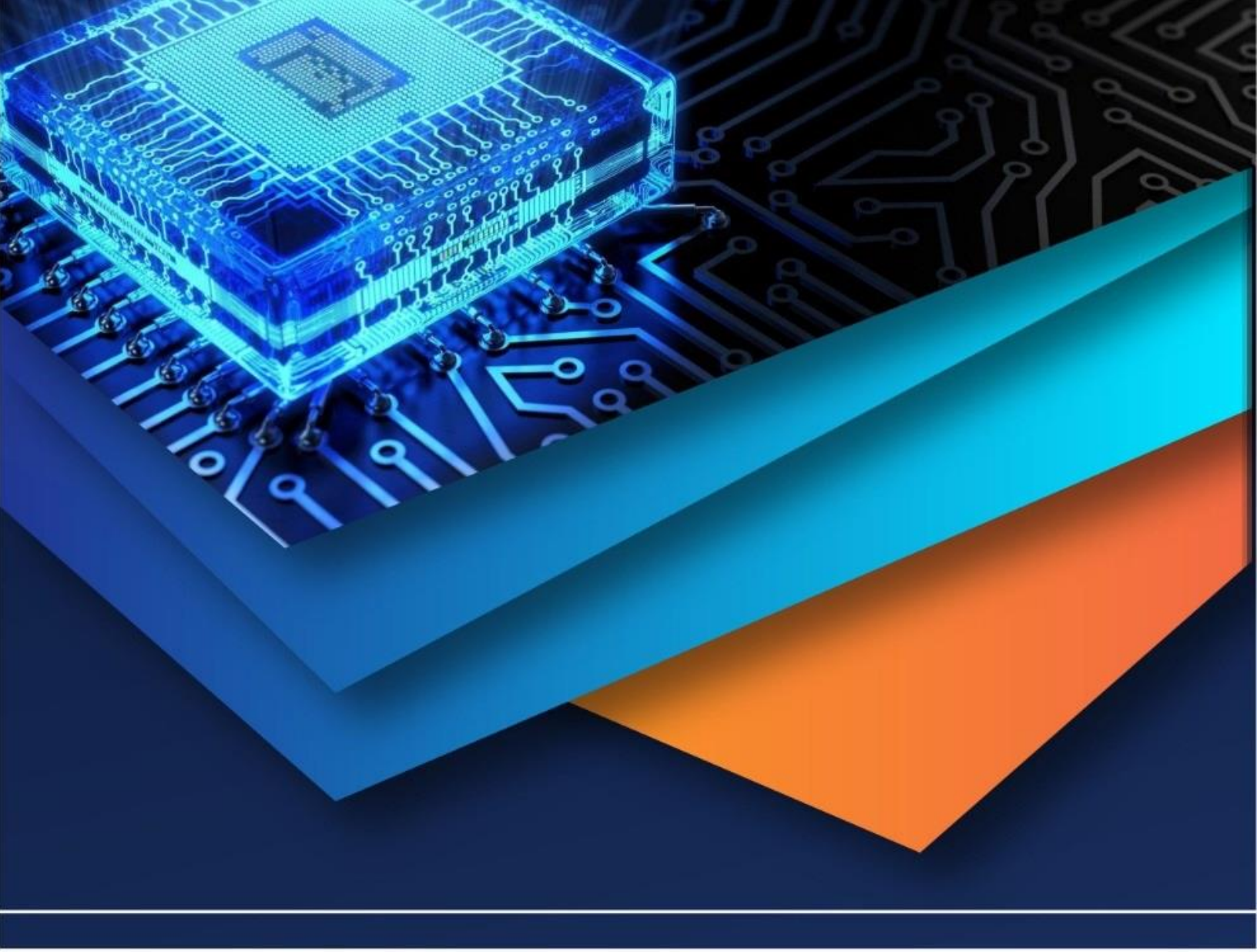
III. CONCLUSION

In this paper, the investigation of the AES algorithm for high-speed and wireless communication applications is studied and presented. It also investigates the sub-byte transformation row shifting column transformation and key expansion processes. The existing AES algorithm is investigated and analyzed in this paper. In order to increase the performance of encryption technologies and ensure security, in the future we will create an AES sub-block with a round key a mixed column and an S-box.

REFERENCES

[1] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "LoRaWAN specification," LoRa Alliance, Tech. Rep., Jan. 2015, pp. 1–82. [Online]. Available: https://lora-alliance.org/resource-hub/lorawanrspecification- v10
[2] Z. Liu, K.-K. R. Choo, and J. Großschädl, "Securing edge devices in the post-quantum Internet of Things using lattice-based cryptography," IEEE Commun. Mag., vol. 56, no. 2, pp. 158–162, Feb. 2018.
[3] D.-H. Bui, D. Puschini, S. Bacles-Min, E. Beigné, and X.-T. Tran, "AES datapath optimization strategies for low-power low-energy multisecuritylevel Internet-of-Things applications," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 12, pp. 3281–3290, Dec. 2017.
[4] C. Patrick and P. Schaumont, "The role of energy in the lightweight cryptographic profile," in Proc. NIST Lightweight Cryptogr. Workshop, 2016, pp. 1–16.
[5] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: A very compact and a threshold implementation of AES," in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn. Tallinn, Estonia: Springer, 2011, pp. 69–88.
[6] T. Järvinen, P. Salmela, P. Hämäläinen, and J. Takala, "Efficient byte permutation realizations for compact AES implementations," in Proc. 13th Eur. Signal Process. Conf., 2005, pp. 1–4.
[7] W. Zhao, Y. Ha, and M. Alioto, "AES architectures for minimum-energy operation and silicon demonstration in 65 nm with lowest energy per encryption," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2015, pp. 2349–2352.
[8] K. Shahbazi, M. Eshghi, and R. Faghih Mirzaee, "Design and implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5," Eng. Sci. Technol., Int. J., vol. 20, no. 4, pp. 1308–1317, Aug. 2017.
[9] L. Ali, I. Aris, F. S. Hossain, and N. Roy, "Design of an ultra-high-speed AES processor for next-generation IT security," Comput. Electr. Eng., vol. 37, no. 6, pp. 1160–1170, Nov. 2011.
[10] A. Soltani and S. Sharifian, "An ultra-high throughput and fully pipelined implementation of AES algorithm on FPGA," Microprocessors Microsyst., vol. 39, no. 7, pp. 480–493, Oct. 2015.
[11] N. Ahmad, R. Hasan, and W. M. Jubadi, "Design of AES S-box using combinational logic optimization," in Proc. IEEE Symp. Ind. Electron. Appl. (ISIEA), Oct. 2010, pp. 696–699.
[12] S. Banik, A. Bogdanov, and F. Regazzoni, "Exploring energy efficiency of lightweight block ciphers," in Proc. Int. Conf. Sel. Areas Cryptogr. Sackville, NB, Canada: Springer, 2015, pp. 178–194.
[13] H. K. Kim and M. H. Sunwoo, "Low power AES using 8-bit and 32-bit datapath optimization for small Internet-of-Things (IoT)," J. Signal Process. Syst., vol. 91, nos. 11–12, pp. 1283–1289, 2019.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)